PRIVACY POLICY

WEALTHDOOR INVESTMENT ADVISERS PRIVATE LIMITED

CHAPTER 1

PREAMBLE

WEALTHDOOR INVESTMENT ADVISERS PRIVATE LIMITED (INA000022057) ("Firm", "Investment Adviser", "RIA", "we", "our" or "us") recognizes that protection of personal information is a fundamental element of investor protection, regulatory compliance, fiduciary responsibility and ethical business conduct.

As a SEBI Registered Investment Adviser, the Firm collects and processes personal information in connection with:

- Client onboarding;
- Risk profiling;
- Suitability assessment;
- Investment advisory services;
- AML compliance;
- KYC verification;
- Regulatory reporting;
- Investor grievance handling;
- Business operations.

The Firm is committed to ensuring that personal information is handled:

- lawfully;
- fairly;
- transparently;
- securely;
- proportionately;
- responsibly.

The Firm has adopted administrative, technical, physical and organizational safeguards designed to protect information from unauthorized access, disclosure, misuse, alteration, destruction or loss.

CHAPTER 2

OBJECTIVES OF THIS POLICY

The objectives of this Policy are:

2.1 Privacy Protection

To protect the privacy rights of clients and other individuals whose information is processed by the Firm.

2.2 Regulatory Compliance

To comply with:

- SEBI (Investment Advisers) Regulations;
- SEBI Master Circular for Investment Advisers;
- Digital Personal Data Protection Act, 2023;
- Information Technology Act, 2000;
- PMLA;
- FATCA and CRS requirements;
- Applicable cybersecurity requirements.

2.3 Transparency

To clearly explain:

- what information is collected;
- why information is collected;
- how information is used;
- who may receive information;
- how long information is retained.

2.4 Information Security

To establish safeguards for protection of personal information.

2.5 Accountability

To ensure accountability for collection, processing, storage and disclosure of personal information.

CHAPTER 3

APPLICABILITY

This Policy applies to:

Clients

Individuals receiving advisory services.

Prospective Clients

Individuals seeking information or considering onboarding.

Website Users

Visitors accessing Firm websites.

Mobile Application Users

Users accessing Firm applications.

Authorized Representatives

Authorized signatories, attorneys and representatives.

Beneficial Owners

Beneficial owners identified pursuant to KYC and AML requirements.

Employees

To the extent employee personal information is processed.

Vendors

Where vendor personnel information is processed.

CHAPTER 4

PRIVACY GOVERNANCE PRINCIPLES

The Firm follows the following privacy principles:

Principle 1 – Lawfulness

Information shall only be processed where there is a lawful basis.

Principle 2 – Fairness

Information shall not be processed in a manner unfair to the individual.

Principle 3 – Transparency

Individuals shall be informed regarding:

- collection;
- usage;
- disclosure;
- retention.

Principle 4 – Purpose Limitation

Information shall only be used for legitimate and disclosed purposes.

Principle 5 – Data Minimization

The Firm shall only collect information necessary for:

- onboarding;
- servicing;
- compliance;
- regulatory requirements.

Collection of excessive information is prohibited.

Principle 6 – Accuracy

Reasonable efforts shall be undertaken to maintain accurate and updated records.

Principle 7 – Storage Limitation

Information shall not be retained longer than necessary.

Principle 8 – Security

Appropriate safeguards shall be implemented to protect information.

Principle 9 – Accountability

The Firm remains accountable for information under its custody or control.

CHAPTER 5

CATEGORIES OF INFORMATION COLLECTED

The Firm may collect the following information.

5.1 Personal Identification Information

Including:

- Full Name;
- Father's Name;
- Mother's Name;
- Date of Birth;
- Gender;
- Nationality;
- Photograph;
- Signature;
- Marital Status.

5.2 Contact Information

Including:

- Residential Address;
- Office Address;
- Correspondence Address;
- Mobile Number;
- Email Address;
- Telephone Number.

5.3 Identity Verification Information

Including:

- PAN;
- Passport;
- Driving Licence;
- Voter ID;
- Aadhaar (where legally permissible);
- OCI Documentation;
- PIO Documentation.

5.4 Financial Information

Including:

- Income Details;
- Net Worth;
- Assets;
- Liabilities;
- Bank Account Details;
- Tax Information;
- Investment Holdings;
- Portfolio Data;
- Source of Funds;
- Source of Wealth.

5.5 Risk Profiling Information

Including:

- Investment Objectives;
- Risk Tolerance;
- Liquidity Requirements;
- Investment Horizon;
- Return Expectations;
- Investment Experience;
- Financial Goals.

5.6 Regulatory Information

Including:

- FATCA Declarations;
- CRS Declarations;
- PEP Information;
- Beneficial Ownership Information;
- AML Documentation.

5.7 Communication Information

Including:

- Emails;
- Call Recordings;

- Video Interactions;
- Meeting Notes;
- Chat Records;
- Service Requests.

5.8 Technical Information

Including:

- IP Address;
- Device Information;
- Browser Information;
- Login History;
- Session Data;
- Application Usage Data.

CHAPTER 6

METHODS OF COLLECTION

Information may be collected through:

Direct Collection

- Client onboarding forms;
- KYC forms;
- Agreements;
- Email communications;
- Physical documents;
- Telephonic interactions.

Digital Collection

- Website forms;
- Mobile applications;
- Client portals;
- CRM systems.

Third Party Sources

- KRA systems;
- Regulatory databases;
- Verification agencies;
- Public records;
- Government databases.

Automated Collection

- Cookies;
- Security logs;
- Application logs;
- Usage analytics.

CHAPTER 7

PURPOSES OF PROCESSING

The Firm may process information for:

a) Client Onboarding
b) KYC Verification
c) Identity Authentication
d) AML Compliance
e) FATCA Compliance
f) CRS Compliance
g) Risk Profiling
h) Suitability Assessment
i) Investment Advisory Services
j) Research Support
k) Client Servicing
l) Complaint Handling
m) Regulatory Reporting
n) Audit Requirements
o) Fraud Prevention
p) Cybersecurity Monitoring
q) Legal Proceedings
r) Business Continuity Planning
s) Disaster Recovery Planning

CHAPTER 8

CONSENT MANAGEMENT FRAMEWORK

The Firm shall obtain consent where required by law.

Consent shall be:

- free;
- informed;
- specific;
- unambiguous.

The Firm shall maintain records of:

- consent obtained;
- consent modified;
- consent withdrawn.

Withdrawal of consent may affect the Firm's ability to provide services.

CHAPTER 9

AI, MACHINE LEARNING AND AUTOMATED PROCESSING

The Firm may utilize:

- Artificial Intelligence;
- Machine Learning;
- Large Language Models;
- Automated Analytics;
- RegTech Solutions.

Such systems may be used for:

- data analysis;
- operational efficiency;
- compliance monitoring;
- report generation;
- research support.

The Firm remains solely responsible for:

- confidentiality;
- security;
- regulatory compliance;
- advisory outputs;
- client suitability obligations.

Client data shall not be uploaded into unauthorized AI systems.